

**Before the  
FEDERAL COMMUNICATIONS COMMISSION  
Washington, D.C. 20554**

**In the Matter of**

**Communications Assistance for Law  
Enforcement Act and Broadband Access and  
Services**

**ET Docket No. 04-295**

**RM-10865**

**To: The Commission**

**COMMENTS OF THE  
UNITED STATES INTERNET SERVICE PROVIDER ASSOCIATION**

## Table of Contents

	<u>Page</u>
I. INTRODUCTION AND SUMMARY .....	1
II. THE SCOPE OF CALEA DOES NOT EXTEND TO “INFORMATION SERVICES” OR PRIVATE NETWORK SERVICES .....	5
A. For Broadband Access Services, the Appropriate Regulatory Distinction Is Between Transmission Services and Internet Services.....	10
B. For VoIP Services, the Appropriate Regulatory Distinction Is Defined by the CALEA Exclusions for “Information Services” (Including “Electronic Messaging Services”) and Private Network Services .....	13
C. The Commission is Correct to Decline to Adopt Rules Applying CALEA to Future Services.....	16
III. CAPABILITY OBLIGATIONS FOR ANY NEWLY REGULATED SERVICES MUST BE CONSISTENT WITH CALEA AND NOT UNDULY BURDENSOME FOR INTERNET SERVICE PROVIDERS .....	16
A. Broadband Access and VoIP Operators Are Required to Deliver Call-Identifying Information Only If It Is “Reasonably Available” .....	17
B. Trusted Third Party Solutions Should Be Subject to the Same Rules as Other CALEA Solutions .....	27
C. The Industry Standards Process Plays the Lead Role in Defining CALEA Capability Requirements.....	30
IV. COMPLIANCE AND ENFORCEMENT ISSUES .....	34
A. The Commission Must Set Realistic Compliance Deadlines .....	34
B. Title III Plainly Authorizes Recovery of CALEA-Related Intercept Costs .....	37
C. The Federal Courts Have Responsibility for CALEA Enforcement .....	41
V. CONCLUSION.....	44
APPENDIX A           Technical Issues for CALEA Compliance for VoIP and Other IP-Based Services	

The United States Internet Service Provider Association (“US ISPA”), a group of the largest Internet service providers (“ISPs”) and Internet portals in the United States, hereby submits these comments in response to the Commission’s Notice of Proposed Rulemaking<sup>1</sup> in this proceeding.<sup>2</sup>

## **I. INTRODUCTION AND SUMMARY**

When the Communications Assistance for Law Enforcement Act (“CALEA”)<sup>3</sup> was enacted in 1994, the role of the Internet in our society and economy was just beginning to become clear, but the Congressional authors of the Act had no difficulty recognizing the potential of the medium:

[Since 1986], society’s patterns of using electronic communications technology have changed dramatically. Millions of people now have electronic mail addresses. Business, nonprofit organizations and political groups conduct their work over the Internet. Individuals maintain a wide range of relationships on-line.<sup>4</sup>

Congress made clear its intent that CALEA would not apply to these new services:

The only entities required to comply with the functional requirements are telecommunications common carriers, the components of the public switched network where law enforcement agencies have always served most of their

---

<sup>1</sup> *In re Communications Assistance for Law Enforcement Act and Broadband Access and Services*, Notice of Proposed Rulemaking and Declaratory Ruling, FCC 04-187, ET Dkt. No. 04-295, RM-10865 (rel. Aug. 9, 2004) (“*CALEA NPRM*”).

<sup>2</sup> The members of US ISPA joining this filing are AOL, BellSouth, MCI, Microsoft, SAVVIS and SBC. EarthLink and Verizon, members of US ISPA, do not join these comments. Many members of US ISPA also will submit individual comments on the NPRM.

<sup>3</sup> Pub. L. 103-414, 108 Stat. 4279 (1994) (codified, as amended, at 18 U.S.C § 2522 and 47 U.S.C. §§ 229, 1001-1010).

<sup>4</sup> H.R. Rep. No. 103-827, 1994 U.S.C.C.A.N. 3489, 3497 (1994) (“*CALEA Legislative History*”).

surveillance orders. ... [E]xcluded from coverage are all information services, such as Internet service providers or services such as Prodigy and America On-Line. All of these ... information services can be wiretapped pursuant to court order, and their owners must co-operate when presented with a wiretap order, but these services and systems do not have to be designed so as to comply with the capability requirements.<sup>5</sup>

Telecommunications and law enforcement have a long history together. But in that history, the direct regulatory approach of CALEA is the exception, not the rule. In fact, apart from CALEA, Congress has never tried to regulate technological innovation on behalf of law enforcement. There are many good reasons for this. On the whole, new technologies have usually provided new sources of evidence, making it possible to solve crimes in new ways. And slowing technological innovation to a pace that law enforcement finds comfortable can have a severe impact on a main source of productivity and competitiveness in the American economy.

During the lengthy debates leading to CALEA's passage, these concerns led Congress to shelve the FBI's sweeping proposals for regulatory authority over telecommunications and to seek a narrower statute that balanced the interests of law enforcement, privacy, and innovation. That balance included three crucial elements. First, the scope of the regulation was carefully limited to services where regulation was most needed and would be least disruptive. Second, the obligations of regulated companies were narrowly focused on capabilities that were crucial to existing investigative techniques. Third, at every turn, the statute left the initiative with industry to find ways to provide those capabilities.

There is no doubt that, since September 11, 2001, maintaining law enforcement's capabilities has new importance for policymakers – and quite properly, too. But that new focus

---

<sup>5</sup> *Id.* at 3498.

does not justify a distortion of CALEA's essential legislative scheme. Congress has enacted many new statutes in response to the events of September 11. If CALEA requires substantial revision, that is a job for Congress too. We join (and incorporate here) earlier filings pointing out how far the *CALEA NPRM* deviates from the statutory text and intention, particularly its assumption that broadband Internet access and Internet telephony are subject to CALEA.<sup>6</sup>

But even if the Commission were starting from scratch with broad authority to revise the statutory scheme and to expand the scope of CALEA to cover new services, it still would face the significant practical constraints that led Congress to impose limits on CALEA. First, there must be some limit to the scope of regulation. There are many technologies that can make the lives of investigators more difficult – *e.g.*, computers can be used to encrypt communications, CD-recorders can be used to transmit detailed criminal plans through the mail, and even iPods could use “podcasting” to download criminal communications from websites. But no one thinks that these technologies, let alone all technologies, should be regulated to reduce the impact on law enforcement. So where is the limit to be drawn? Even if the Commission were

---

<sup>6</sup> The legal concerns of US ISPA in this area are largely those set out in the Comments of the ISP CALEA Coalition (Apr. 12, 2004) in this proceeding. The membership of US ISPA substantially overlaps with the members of that coalition, and that coalition's comments are incorporated by reference into these comments. US ISPA strongly urges that those prior comments be given effect in framing any final rule, not least because a majority of the Commission has already expressed serious concerns with the legal analysis of these issues in the *CALEA NPRM*. See *CALEA NPRM*, Statement of Commissioner Kathleen Q. Abernathy (“it would be a mistake to gloss over the possibility that the existing statutory framework does not apply to broadband Internet access services or other IP-enabled services that are classified as information services.”); *CALEA NPRM*, Statement of Commissioner Michael J. Copps, Concurring (“[The *CALEA NPRM*] is flush with tentative conclusions that stretch the statutory fabric to the point of tear. If these proposals become the rules and reasons we have to defend in court, we may find ourselves making a stand on very shaky ground.”); *CALEA NPRM*, Statement of Commissioner Jonathan S. Adelstein, Concurring (“Rather than seeking comment on the most stable footing for law enforcement's request, the item seizes upon notable but thin distinctions between definitions in CALEA and the Communications Act. Moreover, the item does not acknowledge fully and seek comment on existing precedent that is in tension with the tentative conclusions here.”).

unconstrained by the existing statute, it would have to draw a line that both protects essential law enforcement interests and avoids crippling technological innovation in the United States. Second, any regulatory obligations imposed on fast-moving new technologies must be clear and limited to law enforcement's essential needs. Third, to the greatest extent possible, any regulation should be implemented in a fashion that allows innovation on both technical and business fronts while imposing the costs of regulation on those who receive its benefits.

Even judged purely on these bases, without regard to the legal limits on the Commission's authority to regulate Internet-based services, the scheme set forth in the *CALEA NPRM* is deeply flawed. On all three counts – scope, required capabilities, and implementation – the *CALEA NPRM* proposes a regulatory scheme that runs the risk of drowning innovators in a sea of regulatory uncertainty.

***Scope.*** Because the *CALEA NPRM* proposes to apply CALEA obligations to certain broadband access and voice over Internet protocol (“VoIP”) services that have not previously been subject to Commission regulation, it is critical to address the limit at which CALEA coverage ends and unregulated “information services” begin. In doing so, the Commission must give effect to the CALEA exclusion for “information services,” which includes, in particular, “electronic messaging services.”

***Capability Obligations.*** The nature of CALEA obligations for newly regulated services must be defined with specificity and must only address capabilities that are essential for law enforcement. These US ISPA comments focus on (i) the nature of “call-identifying information” for IP-based services and when it is “reasonably available,” (ii) the role of “trusted third parties,” and (iii) the role of the industry standards process. On the first point, these comments include, at Appendix A, a detailed technical paper explaining the difficulties in the packet-mode

environment with delivering the same call-identifying information that must be delivered under CALEA for circuit-switched communications.

***Implementation/Enforcement.*** These comments also address certain important implementation and enforcement issues: (i) the deadlines for compliance with CALEA obligations for newly regulated services, (ii) the right of providers to include CALEA compliance costs in intercept charges to law enforcement, and (iii) the extent of the Commission's enforcement authority.

## **II. THE SCOPE OF CALEA DOES NOT EXTEND TO “INFORMATION SERVICES” OR PRIVATE NETWORK SERVICES**

Congress squarely faced the problem of how to delineate the border between technologies that are subject to CALEA and those that are not. The text of CALEA explicitly states that the intercept capability requirements of section 103(a) of the statute

do not apply to –

(A) information services; or

(B) equipment, facilities, or services that support the transport or switching of communications for private networks or for the sole purpose of interconnecting telecommunications carriers.<sup>7</sup>

The first of these exclusions, regarding “information services,” is particularly critical.

In the *CALEA NPRM*, the Commission tentatively concluded that CALEA covers certain broadband access and VoIP services even though they are unregulated information services under the Communications Act. This interpretation was based on differences between the definitions of “telecommunications carrier” in CALEA and the Communications Act. Although

---

<sup>7</sup> 47 U.S.C. § 1002(b)(2).

it is true that the definitions in the two statutes are different, that is not a basis for reading the “information services” exclusion out of CALEA, as the Commission proposes to do in the *CALEA NPRM*. The Commission reasoned that, once a service has been classified as a “substantial replacement” for the public switched network, the fact that it is an information service becomes legally irrelevant.<sup>8</sup> This reasoning is clearly wrong on the law.

The Commission’s tentative conclusion rests on the assumption that a service must be either a regulated telecommunications service or an unregulated information service. While this “binary choice” has long been a feature of the Commission’s reading of the Communications Act,<sup>9</sup> there is no reason to believe that Congress incorporated such an approach into CALEA.

In fact, it is very common for statutes to broadly define regulated enterprises or services, subject to specific exceptions from the scope of regulation. For example, the Communications Act defines “common carrier” as “any person engaged as a common carrier for hire, in interstate or foreign communication by wire or radio or interstate or foreign radio transmission of energy...; but a person engaged in radio broadcasting shall not, insofar as such person is so

---

<sup>8</sup> *CALEA NPRM* at ¶ 50.

<sup>9</sup> See, e.g., *In re Telecommunications Carriers’ Use of Customer Proprietary Network Information and Other Customer Information*, Second Report and Order and Further Notice of Proposed Rulemaking, 13 FCC Rcd 8061, 8095-96 ¶ 46 (1998) (“Commission precedent has treated ‘information services’ and ‘telecommunications services’ as separate, non-overlapping categories, so that information services do not constitute ‘telecommunications’ within the meaning of the 1996 Act.”), *vacated on other grounds*, *U.S. West, Inc. v. FCC*, 182 F.3d 1224 (10th Cir. 1999); *In re Federal-State Joint Board on Universal Service*, Report to Congress, 13 FCC Rcd 11501, 11520 ¶ 39 (1998) (“[W]e affirm our prior findings that the categories of ‘telecommunications service’ and ‘information service,’ ... are mutually exclusive.”); *In re Amendment of Section 64.702 of the Commission’s Rules and Regulations (Second Computer Inquiry)*, Final Decision, 77 F.C.C. 2d 384 (1980) (“*Computer II*”) (classifying all services over a telecommunications network as either “basic” or “enhanced”).



engaged, be deemed a common carrier.”<sup>10</sup> Similarly, the Interstate Commerce Act defines “rail carrier” as “a person providing common carrier railroad transportation for compensation, but does not include street, suburban, or interurban electric railways not operated as part of the general system of rail transportation.”<sup>11</sup>

A similar approach makes sense under CALEA – especially because the information services exclusion is a clear and explicit exclusion from CALEA coverage. In contrast, under the Communications Act, information services are not excluded from regulation: the Commission has repeatedly recognized that it is as a matter of discretion that it does not regulate information services under Title I of the Communications Act.<sup>12</sup> The Commission can hardly attach such heavy weight to differing definitions of “telecommunications carrier” without giving

---

<sup>10</sup> 47 U.S.C. § 153(10).

<sup>11</sup> 49 U.S.C. § 10102(5). *See also Dunn v. Commodity Futures Trading Comm’n*, 519 U.S. 465 (1997) (interpreting prior version of Commodity Exchange Act, 7 U.S.C. § 1 *et seq.*, which regulated a general class of investment vehicles known as commodity futures but which excepted certain specific investments such as “transactions in foreign currency”).

<sup>12</sup> *See In re Inquiry Concerning High-Speed Access to the Internet Over Cable and Other Facilities; Internet Over Cable Declaratory Ruling; Appropriate Regulatory Treatment for Broadband Access to the Internet Over Cable Facilities*, Declaratory Ruling and Notice of Proposed Rulemaking, 17 FCC Rcd 4798, 4841 ¶ 76 (2002) (“The Commission asserted ancillary jurisdiction over information services (then called ‘enhanced services’) in the Computer Inquiries. Since then, it has only exercised that authority in limited instances.”) (“*Cable Modem Ruling and NPRM*”); *In re Appropriate Framework for Broadband Access to the Internet over Wireline Facilities; Universal Service Obligations of Broadband Providers; Computer III Further Remand Proceedings: Bell Operating Company Provision of Enhanced Services; 1998 Biennial Regulatory Review - Review of Computer III and ONA Safeguards and Requirements*, Notice of Proposed Rulemaking, 17 FCC Rcd 3019, 3038-39 ¶ 39 (2002) (“The Commission ... found that it possessed jurisdiction over enhanced services under Title I, even as it re-affirmed and bolstered its justification for not imposing common carrier obligations on enhanced service providers. ... It reserved the right to exercise its Title I jurisdiction and to intervene should problems involving enhanced services arise.”) (citing *Computer II*). *See also In re Implementation of Sections 255 and 251(a)(2) of the Communications Act of 1934*, Report and Order and Further Notice of Inquiry, 16 FCC Rcd 6417, 6457 ¶ 98 (1999) (asserting Title I jurisdiction over information services, whether provided by carriers or non-carriers).

effect to this much clearer distinction in the treatment of “information services” between the two statutes.

Even if the Commission were to conclude that a binary approach should apply under CALEA, it cannot simply choose to give effect to the substantial replacement provision and to ignore the information services exclusion. It is a basic principle of statutory construction that “legislative enactments should not be construed to render their provisions mere surplusage.”<sup>13</sup> For example, in *Dunn v. CFTC*, the Supreme Court considered an explicit exemption from the Commodity Exchange Act and reversed an interpretation of it by the Commodity Futures Trading Commission that “would deprive the exemption of the principal effect Congress intended.”<sup>14</sup> Likewise, in the present proceeding, the Commission must read CALEA in a manner that gives full effect to the information services exclusion, even where the substantial replacement provision is applied.

In fact, after making much of differences in how the Communications Act and CALEA define telecommunications service, the *CALEA NPRM* fails to take account of an equally striking difference in the two acts’ definitions of “information services.” CALEA’s definition incorporates almost verbatim the definition found in section 153(20) of the Communications Act,<sup>15</sup> except that CALEA expressly includes “electronic messaging services” within the definition of “information services.” This strongly suggests that, if anything, Congress intended

---

<sup>13</sup> *Dunn*, 519 U.S. at 472. See also, e.g., *Mountain States Tel. & Tel. Co. v. Pueblo of Santa Ana*, 472 U.S. 237, 239 (1985) (finding it is an “elementary canon of construction that a statute should be interpreted so as not to render one part inoperative”).

<sup>14</sup> *Dunn*, 519 U.S. at 471.

<sup>15</sup> 47 U.S.C. § 153(20).

the information services exception in CALEA to be given a broader reading than the same term in the Communications Act. Certainly the Commission cannot properly focus on differences between definitions of “telecommunications carrier” in the Communications Act and CALEA while failing to consider the two statutes’ definitions of “information services.”

Moreover, the Commission’s own reasoning in the *CALEA NPRM* does not support its treatment of the information services exclusion. The Commission states that “the history and purposes of CALEA support [its] interpretation” that the information services exclusion has limited effect.<sup>16</sup> The primary evidence the Commission offers on this point, however, is that the text and legislative history of CALEA indicate that the transmission component of Internet-based services may be regulated, while the ISP services provided via such transmission are exempt.<sup>17</sup> US ISPA agrees with this transmission / content distinction (see section II.A below), but the distinction in no way supports the Commission’s effort to relegate the information services exclusion to irrelevance. To the contrary, the transmission / content distinction indicates that an entity that is a telecommunications carrier under CALEA also may provide unregulated information services.

In sum, CALEA manifestly requires the Commission to draw a principled line between telecommunications services covered by CALEA and exempt information services. It is particularly important for the Commission to take care in this task, given that it is now proposing to expand its mandate to regulate services that have previously been unregulated under both the Communications Act and CALEA. The remainder of this section proposes methods of

---

<sup>16</sup> *CALEA NPRM* at ¶ 50

<sup>17</sup> *Id.* at ¶¶ 51-52.

determining which services are covered by CALEA that can be squared with the text and legislative history of CALEA.

**A. For Broadband Access Services, the Appropriate Regulatory Distinction Is Between Transmission Services and Internet Services**

As the Commission has recognized in the *CALEA NPRM*, CALEA draws a clear distinction between telecommunications transmission services used to access the Internet on the one hand, and “the ISP providing e-mail, content, web hosting and other Internet services”<sup>18</sup> on the other hand. The Commission’s “tentative conclusion [to draw this distinction] respects Congress’s understanding and does not propose attaching CALEA obligations to services or applications that ‘ride over’ the underlying broadband transmission, such as e-mail storage, web browsing capabilities, and Internet gaming.”<sup>19</sup> US ISPA strongly supports this tentative conclusion. At the same time, the border between what is regulated and what is not regulated must be defined with great precision. Law enforcement will always have an incentive to move the border – to attempt to assert authority over unregulated as well as regulated technologies. As a result, even unregulated technologies could face heavy regulatory costs if the border is not defined with precision.

Drawing a regulatory distinction between broadband transmission services and Internet services that “ride over” such services is consistent with the Commission’s prior jurisprudence. In the *CALEA Second Report and Order*,<sup>20</sup> the Commission explained that “[w]here facilities are

---

<sup>18</sup> *Id.* at ¶ 51.

<sup>19</sup> *Id.*

<sup>20</sup> *In re Communications Assistance for Law Enforcement Act*, Second Report and Order, 15 FCC Rcd 7105 (1999) (“*CALEA Second Report and Order*”).

used to provide both telecommunications and information services, ... such joint use facilities are subject to CALEA in order to ensure the ability to surveil the telecommunications service” but not the information service.<sup>21</sup> Likewise, in the *Wireline Broadband NPRM*,<sup>22</sup> the Commission distinguished between “the transmission component of retail wireline broadband Internet access service” (which it considered to be “telecommunications,” but not a “telecommunications service”)<sup>23</sup> and the “capability for generating, acquiring, storing, transforming, processing, retrieving, utilizing or making available information *via telecommunications*.”<sup>24</sup> In short, the legal authority establishing the distinction between the transmission component and the Internet services component of broadband access services – both under CALEA and under the Communications Act – is consistent and clear.

In order to implement the transmission / Internet services distinction effectively, the Commission in this proceeding must carefully clarify the scope of broadband transmission services that it proposes to regulate under CALEA. US ISPA proposes that any CALEA obligations be limited to ***facilities-based telecommunications transmission services that are a component of broadband access services***. This definition implements the transmission / Internet

---

<sup>21</sup> *Id.* at 7120 ¶ 27.

<sup>22</sup> *In re Appropriate Framework for Broadband Access to the Internet over Wireline Facilities*, Notice of Proposed Rulemaking, 17 FCC Rcd 3019 (2002) (“*Wireline Broadband NPRM*”).

<sup>23</sup> *Id.* at 3029 ¶ 17.

<sup>24</sup> *Id.* at 3030 ¶ 19 (quoting Communications Act definition of “information service”) (original emphasis). See also *Cable Modem Ruling and NPRM* at 4820. In reviewing the Commission’s analysis of this issue in the context of cable modem service, the Ninth Circuit Court of Appeals in *Brand X Internet Services v. FCC* reached the same conclusion that the Commission has reached under CALEA in the present NPRM – *i.e.*, “that cable broadband service ... [is] part ‘telecommunications service’ and part ‘information service.’” 345 F.3d 1120, 1132 (9th Cir. 2003). See also *AT&T v. City of Portland*, 216 F.3d 871 (9th Cir. 2000). US ISPA expresses no view on whether the regulatory analysis of *Brand X* is correct under the Communications Act.

services distinction and reflects the Commission's proper recognition that only facilities-based service providers have access to the information required for compliance with CALEA obligations.<sup>25</sup>

Likewise, the Commission should specify the components of broadband access services that are not regulated under CALEA. First, and most important, CALEA plainly does not regulate pure Internet services – *i.e.*, applications and content, either within the network of an ISP or Internet portal providing the broadband access service, or within the home or business network of the subscriber. Both such services fall within the information services exclusion of CALEA and outside the substantial replacement provision of CALEA – even under the exceptionally broad definition of “switching” proposed in the *CALEA NPRM*:

[W]e interpret “switching” ... to include routers, softswitches, and other equipment that may provide addressing and intelligence functions for packet-based communications to manage and direct the communications along to their intended destinations.<sup>26</sup>

Traffic within either a home network or an ISP network is certainly already at its “destination” for purposes of this definition.

The Commission also should conclude that the Internet backbone is not covered by CALEA. It is established that CALEA does not apply to circuit-mode long distance networks,<sup>27</sup> and the Internet backbone is the IP equivalent of long distance carriage. Furthermore, the

---

<sup>25</sup> *CALEA NPRM* at ¶ 47 (“[W]e tentatively conclude that facilities-based providers of any type of broadband Internet access ... are subject to CALEA (with possible limited exception ...)”).

<sup>26</sup> *Id.* at ¶ 43. US ISPA does not agree that such a broad definition of “switching” is supported by the language of CALEA or by Commission precedent.

<sup>27</sup> *CALEA Legislative History* at 3498 (“[S]ervices that support the transport or switching of communications for private networks or for the sole purpose of interconnecting telecommunications carriers (these would include long-distance carriage) need not meet any ... wiretap standards”).

backbone is not an appropriate place to conduct effective wiretaps because backbone providers typically do not serve end customers and they route high volumes of traffic at protocol layers below those of VoIP (and other communications of potential interest to law enforcement). As a result of these factors, the technical difficulties with packet-mode intercepts that are discussed in Appendix A (including the difficulty of “breaking open” packets) are particularly significant.

**B. For VoIP Services, the Appropriate Regulatory Distinction Is Defined by the CALEA Exclusions for “Information Services” (Including “Electronic Messaging Services”) and Private Network Services**

Just as the line between covered telecommunications and exempt information services should be defined with great clarity in the context of broadband services, so too the Commission must clearly define which VoIP services are regulated under CALEA. This is a particularly difficult task given the rapidly developing and diversifying VoIP market and the lack of any clear industry definition of what constitutes “VoIP.” Unfortunately, the distinction offered in the *CALEA NPRM* between “managed” and “unmanaged” VoIP services<sup>28</sup> is, well, unmanageable. Instead, the Commission should distinguish between regulated and unregulated VoIP services under CALEA by using the statutory exclusions for “information services” and private network services.

The Commission proposes to define “managed” VoIP services as those “offered to the general public as a means of communicating with any telephone subscriber, including parties reachable only through the PSTN.”<sup>29</sup> US ISPA understands why the Commission views services

---

<sup>28</sup> *CALEA NPRM* at ¶¶ 56-58.

<sup>29</sup> *Id.* at ¶ 56.

that meet this description as the strongest candidates for CALEA coverage.<sup>30</sup> The reasons have almost nothing to do with whether the services are “managed,” however. What’s more, making the border between CALEA regulation and exemption turn on whether the service is “managed” will create great confusion. All private networks are “managed,” many private networks connect to the PSTN, and, indeed, the *CALEA NPRM* clearly states that private networks (such as “voice-enabled Instant Messaging” networks) are exempt from CALEA.<sup>31</sup> Does that subject them to CALEA, notwithstanding the clear Congressional intent to the contrary? Inevitably, adopting such a line will set the stage for years of unwarranted conflict over private networks.

The *CALEA NPRM* compounds the confusion by suggesting that “non-managed” communications are “disintermediated ... communications.”<sup>32</sup> Again, this definition is highly confusing and risks retracting the clear exemption for “voice-enabled Instant Messaging”<sup>33</sup> as an information service. This is because Instant Messaging of all kinds depends heavily on central servers for management of communications.

The emphasis on whether communications are “managed” also may lead to confusion in the other direction. Some VoIP services that the Commission evidently intends to cover may use central servers only for initiation of calls (*e.g.*, using session initiation protocol (“SIP”)), while call termination on the PSTN and otherwise is widely distributed among numerous servers in the geographical locations where calls are terminated (not unlike a peer-to-peer model). In sum,

---

<sup>30</sup> US ISPA does not agree with (but does not address here) the Commission’s conclusion that such services already satisfy the substantial replacement provision of CALEA.

<sup>31</sup> *CALEA NPRM* at ¶ 58.

<sup>32</sup> *Id.*

<sup>33</sup> *Id.*



numerous variations in VoIP architecture are possible; and deciding which are “managed” and which are “non-managed” is certain to be a regulatory morass.

Rather than taking the ambiguous managed / non-managed approach, the Commission should take its guidance from the language of CALEA. First, CALEA exempts “information services,” including “electronic messaging services,” which it defines as

software-based services that enable the sharing of data, images, sound, writing, or other information among computing devices controlled by the senders or recipients of the messages.<sup>34</sup>

In recognizing that peer-to-peer services, as well as voice-enabled Instant Messaging, are not covered by CALEA, the Commission should ground its ruling in the plain language of this provision. Second, CALEA exempts “equipment, facilities, or services that support the transport or switching of communications for private networks.”<sup>35</sup> Accordingly, to the extent that any VoIP services become subject to CALEA, the Commission should define the VoIP services covered by CALEA to include ***IP-based voice services that are offered to the general public for a fee and do not fall within the CALEA exclusions for “information services” and/or private network services.*** Unlike the “managed” / “non-managed” distinction, application of these exclusions to VoIP services would provide a framework based on actual functionality delivered to end users, rather than on the particular technological approach selected.

Fortunately, the *CALEA NPRM* does not rely exclusively on “management” to define the line between covered and exempt VoIP. Elsewhere, the Commission explicitly relies on the two statutory exemptions discussed above:

---

<sup>34</sup> 47 U.S.C. § 1001(4).

<sup>35</sup> *Id.* at § 1002(b)(2)(B).

Non-managed VoIP services ... do not appear to be subject to CALEA for two reasons. First, because they are confined to a limited universe of users solely within the Internet or a private IP-network, they may be more akin to private networks, which Congress expressly excluded from section 103's capability requirements. Therefore, they do not appear to replace a substantial portion of local exchange service; as such they do not appear to fall within the Substantial Replacement Provision. Second, they may be excluded information services under section 103(b)(2)(A).<sup>36</sup>

US ISPA strongly supports this line of reasoning, and it urges the Commission to drop any reliance on the "managed" / "non-managed" distinction, which will lead to great confusion in the long run.

**C. The Commission is Correct to Decline to Adopt Rules Applying CALEA to Future Services**

US ISPA also strongly supports the Commission's tentative conclusion that it should not adopt rules for application of CALEA to future services based upon its concern "that the proposed approach could be inconsistent with the statutory intent and could create an obstacle to innovation."<sup>37</sup> Under any reasonable reading of CALEA, this concern is dispositive. Accordingly, the Commission should uphold its tentative conclusion.

**III. CAPABILITY OBLIGATIONS FOR ANY NEWLY REGULATED SERVICES MUST BE CONSISTENT WITH CALEA AND NOT UNDULY BURDENSOME FOR INTERNET SERVICE PROVIDERS**

In constructing a regulatory scheme for new technologies, the Commission must be clear not only about the technologies that are covered but also about the obligations being imposed.

---

<sup>36</sup> *CALEA NPRM* at ¶ 58.

<sup>37</sup> *Id.* at ¶ 61.

The extension of CALEA to certain broadband access and VoIP services will greatly expand the jurisdiction of the Commission over services that previously have not been regulated, either under the Communications Act or CALEA. This rising tide of CALEA coverage is at odds with the Commission's general policy of light-handed regulation of the Internet.<sup>38</sup> Accordingly, it is critical that the CALEA capability obligations identified by the Commission be (1) limited to those that are plainly required by CALEA and (2) not unduly burdensome on ISPs and Internet portals that have not previously faced telecommunications regulation. On both points, the Commission must carefully balance law enforcement interests against the goals of Congress "to protect privacy in the face of increasingly powerful and personally revealing technologies; and ... to avoid impeding the development of new communications services and technologies."<sup>39</sup>

**A. Broadband Access and VoIP Operators Are Required to Deliver Call-Identifying Information Only If It Is "Reasonably Available"**

Generally, industry and law enforcement agree that the capability requirements under section 103(a) of CALEA include the delivery of communication *content* for regulated services. Indeed, despite the concerns raised by law enforcement about allegedly wiretap-proof

---

<sup>38</sup> See, e.g., *In re Petition for Declaratory Ruling that pulver.com's Free World Dialup is Neither Telecommunications Nor a Telecommunications Service*, Memorandum Opinion and Order, FCC 04-27, WC Dkt. No. 03-45, ¶ 1 (Feb. 19, 2004) ("We formalize the Commission's policy of nonregulation to ensure that Internet applications remain fully insulated from unnecessary and harmful economic regulation at both the federal and state levels."); Federal Communications Commission, Consumer & Governmental Affairs Bureau, *Voice Over Internet Protocol*, available at <http://www.fcc.gov/voip/> (last updated June 23, 2004) ("Historically, the FCC has not regulated the Internet or the services provided over it."); *Press Statement of Commissioner Michael Powell on the Approval of AOL-Time Warner Merger* (Jan. 23, 2001) ("[T]he Commission, for decades now, has expressly declined to regulate similar computer, data processing and information services for the very reason that such interference would undermine the energy and drive toward innovation that characterizes these highly competitive markets.").

<sup>39</sup> *CALEA Legislative History* at 3493.

technologies, virtually all technologies being implemented today allow access to the content of subscriber communications.

The principal areas of dispute between industry and law enforcement regarding CALEA capability obligations relate instead to the delivery and scope of “call-identifying information” (“CII”). CII is valuable to law enforcement – and law enforcement agencies are of course free to analyze packet streams delivered to them pursuant to CALEA in order to extract CII. But the CALEA obligation for carriers is narrower for CII than for content. Under CALEA, a carrier must isolate and deliver to law enforcement all call content but only the CII that is “reasonably available” to it.<sup>40</sup>

In extending CALEA to new technologies, the Commission should exercise great care to impose only obligations that are clear and essential to the Commission’s goals. There is nothing essential about imposing a broad or vague obligation to deliver CII in the context of broadband access or VoIP. Once access to call content has been assured, CII may be valuable, but it is rarely essential. At the same time, any lack of clarity in defining the CII that carriers must provide will add greatly to regulatory uncertainty. That is particularly so because the Commission’s only definition of CII has been in the context of circuit-switched communications, where call signaling has long been standardized. To avoid confusion and burdens on Internet-based operators, the Commission should set a clear standard for CII that is applicable to a broad range of technologies. The alternative is an endless string of disputes about how to translate the Commission’s circuit-switched definitions of CII into new technological environments.

---

<sup>40</sup> 47 U.S.C. § 1002(a)(2).

US ISPA submits that the natural reading of the statute is that CII is “reasonably available” to a carrier only if it is used by the carrier in the course of serving the carrier’s customers. Such a standard also would be consistent with the Commission’s responsibility to ensure that CALEA standards meet the assistance capability requirements “by cost-effective methods” and also “protect the privacy and security of communications not authorized to be intercepted”<sup>41</sup> – particularly in the context of packet-mode services and technologies. Any requirement to provide information not used by the carrier is likely to create a *de facto* requirement to extract CII by “breaking open” packets – *i.e.*, a requirement to examine the parts of the packet that are not ordinarily examined or used by the carrier. This would require significant network modifications, impose an undue burden on carriers, and raise significant security concerns, as described below and in Appendix A of these comments.

In its decisions on CALEA obligations in the circuit-mode context, the Commission has not consistently limited the phrase “reasonably available” to information used in a carrier’s ordinary operations; it has occasionally required carriers to deliver various other CII. But it has set forth important constraints on the CII that must be delivered. In the *CALEA Third Report and Order*, the Commission decided that CII must be delivered only if it is “present at a carrier’s IAP [intercept access point] and can be made available without the carrier being unduly burdened with network modifications.”<sup>42</sup>

In the *CALEA NPRM*, the Commission tentatively concludes that it “should apply the same criteria – *i.e.*, information may not be ‘reasonably’ available if the information is only

---

<sup>41</sup> 47 U.S.C. § 1006(b)(1), (2).

<sup>42</sup> *In re Communications Assistance for Law Enforcement Act*, Third Report and Order, 14 FCC Rcd 16794, 16808 ¶ 28 (1999) (“*CALEA Third Report and Order*”).

accessible by significantly modifying a network – to broadband access and VoIP providers.”<sup>43</sup> While US ISPA agrees that, at a minimum, these constraints should continue to apply, their application to IP networks is uncertain. After all, so long as a stream of packets is flowing through a company’s network, it has access (in theory) to those packets. The problem is not access to the stream, as it was in the Commission’s other decisions, but whether the carrier will be forced to open up each packet in the stream to find information that it does not use and usually will not understand. Moreover, as explained in more detail in Appendix A, the carrier may be unable to determine if the packet is actually covered by CALEA or within the scope of an electronic surveillance order (e.g., port spoofing – misidentifying the packet’s port of origin or destination – could cause a carrier to fail to isolate relevant CII or to mistakenly deliver CII not associated with a covered service), making compliance difficult or impossible. These are serious concerns that cannot easily be fit into the rubric of “network modification.” For that reason, US ISPA urges the Commission to adopt the clearer and simpler test – limiting CII to information that the carrier routinely uses in delivering services to the subscriber.

This position is reinforced by concerns about excessive regulatory burden on new technologies. The cost to a carrier of delivering CII not used in its operations is a critical aspect of assessing whether that CII is “reasonably available.” In the *CALEA Third Report and Order*, the Commission concluded that “[i]n addition to network design considerations, ... cost and privacy considerations [are] to be considered in determining whether call-identifying information is ‘reasonably available’ to an originating carrier.”<sup>44</sup> However, the Commission has more

---

<sup>43</sup> *CALEA NPRM* at ¶ 68.

<sup>44</sup> *CALEA Third Report and Order* at 16809 ¶ 29.

recently wavered from this approach, stating in its *CALEA Order on Remand*<sup>45</sup> that “we think cost concerns are better addressed as part of our Section 107(b) analysis, as opposed to our inquiry as to whether information is ‘reasonably available’ to a carrier”,<sup>46</sup> and the *CALEA NPRM* echoes this analysis.<sup>47</sup> This more recent line of reasoning is inconsistent with the structure of CALEA.

Under CALEA, the Commission may consider whether CII is “reasonably available” *only* in the context of a petition under section 107(b). That section states that if the industry does not develop standards for CALEA compliance and the Commission instead develops a standard, such standard or technical requirements must meet section 103’s capability requirements “by cost-effective methods.” This constraint cannot be ignored simply because the Commission in this proceeding appears to want to conduct a general rulemaking on the meaning of “reasonably available.” More generally, it simply cannot be the case that CII not used by the carrier in its operations is “reasonably available” no matter what the cost to the carrier of providing it.

In applying these principles to define capability obligations for broadband access and VoIP services, it is critical to consider, as stated in the *CALEA NPRM*, that “[p]acket technologies are fundamentally different from the circuit switched technologies that were the primary focus of the Commission’s earlier decisions on CALEA.”<sup>48</sup> The CII that is generated and received by packet networks is very different from the CII generated and received by a

---

<sup>45</sup> *In re Communications Assistance for Law Enforcement Act*, Order on Remand, 17 FCC Rcd 6896 (2002) (“*CALEA Order on Remand*”).

<sup>46</sup> *Id.* at 6927.

<sup>47</sup> *CALEA NPRM* at ¶ 67.

<sup>48</sup> *Id.* at ¶ 63.

traditional circuit-switched network.<sup>49</sup> Consequently, findings about the kinds of CII that are “reasonably available” to carriers operating circuit-switched networks cannot and should not control or determine the CII that is “reasonably available” to carriers operating packet networks. Most significantly, retrieval in the packet-mode context of CII like that on circuit-mode networks (*e.g.*, as specified in J-STD-025A) could require carriers (in particular, broadband access providers) to “break open” packets and examine packet content and header information at network layers not under their control.

The problem of separating CII from content in the packet context is well recognized. As the Commission has explained:

Call-identifying information [for packet technologies] may be found within several encapsulated layers of protocols ... . As the packet makes its way through the network of the broadband access service and Internet service providers, these providers’ equipment generally do not examine or process information in the layers used to control packet-mode services such as VoIP ... . As a result, the broadband access service and Internet service providers may not be able to easily isolate call-identifying information for VoIP without examining the packet in detail, or in other words, examining the packet content.<sup>50</sup>

Because of these circumstances, it would be highly burdensome and would require major network modifications for packet-mode carriers to “break open” packets to extract CII when such information is not routinely examined or processed by the carrier. In various cases, CII that must be provided in the circuit-mode context would not be available at all. These issues are discussed in technical detail in Appendix A to these comments. In brief, the major issues are as follows.

---

<sup>49</sup> *Id.* at ¶ 66.

<sup>50</sup> *Id.* at ¶ 65.



*First*, as recognized by the Commission in the above block quote, isolating CII is a challenge because a carrier may process packets at a different protocol layer than the one that is of interest to law enforcement. If a single service provider handles every protocol layer of a packet-mode communication, then it generally would be able to isolate information of interest to law enforcement. But this is rarely the case. Internet services are designed to be vertically dis-integrated, and multiple providers are involved and in control of different protocol layers for almost all services. In such an environment, a broadband service provider that ordinarily would do nothing more than carry IP-based communications may lack critical information relating to communications at a different protocol layer – including the identity of the protocols used in that layer and “state” information regarding the protocols that are maintained by the communicating parties – making it difficult for that service provider to interpret and extract the information in the protocol layers not within its control.

For example, as more fully described in Appendix A, VoIP service typically involves the use of Session Initiation Protocol (“SIP”) for call set-up, management, and termination, and the use of Real Time Protocol (“RTP”) for call content. Both SIP and RTP packets contain three separate layers of headers, and a broadband access provider typically processes only the IP header. Furthermore, there are many variations in how VoIP can be provided by multiple service providers with varying control over SIP and RTP packet streams:

- A user may obtain broadband access service from one provider and VoIP service from another. The two providers would process entirely different sets of packet headers.
- The user’s VoIP provider may be a pure reseller of another provider’s wholesale VoIP service or may perform some of the signaling functions before handing off the VoIP traffic to a wholesale VoIP provider for transport and call completion. Depending on the division of responsibilities, different call signaling information may be processed by the VoIP wholesaler and retailer.

- A VoIP provider also may do no more than help negotiate an IP-to-IP call between users, but then never see any call content because the call is being transported by other providers' IP networks.

In other words, different entities in the broadband access and VoIP service supply chain have different access to CII and call content information. It is therefore simplest and most cost effective for law enforcement to obtain the relevant information from the service provider that actually uses or processes that information. The statute is not meant to be a substitute for the most effective law enforcement technique of all – old-fashioned shoe leather. The CALEA obligations of service providers should not be expanded simply to save law enforcement from having to obtain data from multiple service providers when no service provider has access to all of the information that law enforcement wants.

*Second*, the high-speed IP routers that broadband access providers and Internet service providers ordinarily employ are designed to do no more than read packet headers and route them in accordance with their routing tables. Routers would have to be significantly modified and redesigned to “break open” the packet, examine the contents, determine whether any of the content is CII associated with a CALEA-covered service that the user may or may not be running, and then replicate and deliver that information to law enforcement.<sup>51</sup> Modifying routers to extract such information could severely affect their performance (*i.e.*, the speed at which they routes packets) and thus degrade the overall performance of the network – possibly necessitating further network modifications to compensate for this delay. Technical solutions to these issues

---

<sup>51</sup> Somewhat less significant modifications to the router itself would be required in order to “split” the packet stream, by sending one copy to the recipient address and one copy to a separate CALEA analysis system. But development of that analysis system would involve similar technical challenges to those involved in router modification, and these challenges are considerable for a high-speed packet stream.

are emerging, but the highly technical and complex nature of such solutions (and the complexity of their interactions with existing networks) strongly reinforces the point that it is industry that must provide leadership in designing the standards and solutions for CALEA compliance.

*Third*, unlike circuit-switched networks, most of the processing intelligence in the Internet and other IP networks is located on the network edges rather than in the network core. Compared with central office switches in the circuit-switched world, IP switches and routers perform fairly simple tasks; and “intelligence” is implemented primarily at the network edge by end-user software or equipment. For example, the SIP phones and special terminal adaptors that VoIP customers purchase often have call waiting, call hold, call forwarding, and three-way calling capabilities built in. When a user activates one of these features, the customer equipment provides all of the functionality, and no signaling information is transmitted to or under the control of the carrier. On this issue, the Commission should confirm its earlier conclusion that “[w]hen customer premises equipment is used to perform any of [these] functions ... and no network signal is generated, that information is not reasonably available to a carrier, and thus is not required to be provided.”<sup>52</sup>

*Fourth*, many packet-based communications use some form of encryption, either of the overall packet stream (*e.g.*, using IPSec) or of particular content (*e.g.*, using SSL). Where the carrier does not provide the encryption functionality (or lacks the information to decrypt the communications – *e.g.*, because encryption keys are under end-user control), CALEA provides that there is no obligation to deliver decrypted call content or CII.<sup>53</sup> Furthermore, it may be

---

<sup>52</sup> *CALEA Order on Remand* at 6936 ¶ 108.

<sup>53</sup> 47 U.S.C. § 1002(b)(3).

difficult or impossible for a carrier to tell whether information at a higher protocol layer is unintelligible because of use of encryption or because the carrier lacks essential protocol information (as discussed above). CALEA imposes no obligation for the carrier to resolve this technical dilemma where it has no operational need to process the information in question.

In addition to these technical issues, giving routers the capability to “break open” packets creates serious security concerns. Deliberately creating “backdoors” that would enable packets to be examined and diverted will make packet networks less secure and will increase their susceptibility to hacking. Hackers have been known to break into the circuit switches of telephone carriers, and there is nothing to suggest that this could not also be done with respect to IP routers that have intercept capabilities built in. Any CALEA standard for broadband access and VoIP services will need to address these concerns.

Finally, a few items that the *CALEA NPRM* identifies as potentially being CII deserve particular attention. First, dialed digit extraction (“DDE”) is far more complex on a packet network. On a circuit-mode network, carriers may not have a business reason to process post-cut-through dialed digits,<sup>54</sup> but the dialed digits are at least transmitted by the network – typically as dual tone multi-frequency (“DTMF”) tones – and can be captured through installation of additional tone decoders and associated software in central office switches. By contrast, on a packet network, tones and other information on the voice channel are encoded as a string of bits, in a manner depending entirely upon the protocols and other functionality of hardware or software controlled by end users. In many cases, it is likely to be literally impossible for DDE

---

<sup>54</sup> See generally *CALEA Order on Remand* at 6921-32.

information to be extracted from a stream of IP packets. For these reasons, DDE in packet networks is not “reasonably available” CII.<sup>55</sup>

Second, the *CALEA NPRM* suggests that CII includes “information about changes to the subject’s service or account profile, which could include, for example, new or changed logins and passwords.”<sup>56</sup> ISP login information (and account information more generally) does not meet the definition of CII because it does not “identif[y] the origin, direction, destination, or termination” of any communication that is covered by CALEA.<sup>57</sup> Rather, login information authenticates a user prior to using ISP information services that are plainly exempt from CALEA. Furthermore, a broadband access provider would face many of the technical challenges noted above in seeking to provide such information.

**B. Trusted Third Party Solutions Should Be Subject to the Same Rules as Other CALEA Solutions**

The Commission’s “trusted third party” (“TTP”) approach has the potential benefit of offering efficient CALEA compliance solutions for providers and law enforcement, thereby relieving service providers of the obligation to build their own solution. Government-sanctioned TTP solutions also raise significant concerns, however, including introducing new risks to the privacy and security of communications and distorting CALEA capability requirements. The proper way to address these concerns is simply to maintain the *status quo* by permitting TTP solutions but not giving them any special status under CALEA.

---

<sup>55</sup> See *CALEA NPRM* at ¶ 83.

<sup>56</sup> *Id.* at ¶ 66.

<sup>57</sup> 47 U.S.C. § 1001(2).

The use of a third party to extract the content and CII of packet communications raises substantial concerns about data privacy and security. Essentially, TTPs (and communications between carriers and TTPs) would be a new and significant potential point of failure from an information security perspective – producing increased risks of both unintentional security failures and intentional attacks. Communication service providers would be obliged to conduct careful due diligence on the security and privacy practices of potential TTPs and to negotiate data privacy agreements with them. Furthermore, for any third party system to work – and to remain commercially viable – it would need to be connected to the infrastructure of multiple providers and would need to have access to the providers’ infrastructures. This situation would both increase the risk of improper or illegal sharing of information and would produce a particularly attractive target for hackers – or even foreign governments. Although hacking and security are concerns with which US ISPA members are familiar (and know how to mitigate) the ability to do so depends upon having flexibility in managing network configuration in order to deal with the risks. Any mandate for a TTP approach would eliminate this flexibility.

Giving special status to TTP solutions also would impair the safe harbor under section 107(a) of CALEA. The Commission recognizes this danger when it acknowledges in the *CALEA NPRM* that there is a “tension between relying on a trusted third party model and relying on ‘safe harbor’ standards.”<sup>58</sup> Of chief concern is the possibility that one or more TTPs could seek to gain market share (and improve profitability) by adding non-CALEA features to their services in order to become favorite partners of law enforcement. If the Commission were to require (or give preferential status to) such TTP solutions, providers would be forced to provide

---

<sup>58</sup> *CALEA NPRM* at ¶ 73.

more than CALEA requires, and to pay whatever the TTPs charge, in order to avoid an enforcement action. In other words, the Commission should not conclude that particular CII is “reasonably available” simply because an aspiring TTP has announced a willingness to extract it as part of a high-priced solution. Giving TTPs this sort of authority effectively would take the section 107(a) standards process – a part of CALEA that has so far functioned more or less as Congress intended – and turn it over to the control of TTPs and law enforcement.

It ultimately may make sense for TTPs to be “owned by ... Law Enforcement,” as suggested in the *CALEA NPRM*,<sup>59</sup> or at least for law enforcement to pay the costs of establishing and running one or more TTPs. There is no doubt that smaller law enforcement agencies will be daunted by the complexity of obtaining wiretap connections to multiple providers; and the long-term solution may well be the establishment of TTPs that can provide connections and a variety of “translation” services to local law enforcement. But to give TTPs affiliated with government a special role in defining CALEA compliance would flatly contradict the prohibitions of CALEA section 103(b)(1): law enforcement may not “require any specific design of equipment, facilities, services, features, or system configurations” or “prohibit the adoption of any equipment, facility, service, or feature by any provider of a wire or electronic communication service.”<sup>60</sup>

Fortunately, the Commission can address these concerns regarding the TTP approach simply by maintaining the *status quo*. The offerings of TTPs will continue to be attractive if they

---

<sup>59</sup> *Id.* at ¶ 75.

<sup>60</sup> 47 U.S.C. § 1002(b)(1). *See also CALEA Legislative History* at 3499 (“The bill expressly provides that law enforcement may not dictate system design features and may not bar introduction of new features and technologies ... . This is the exact opposite of the original versions of the legislation, which would have barred introduction of services or features that could not be tapped.”).

provide cost-effective capabilities that implement CALEA compliance solutions based on industry standards. Therefore, TTP solutions should be permitted, but they should not be required and should have no special status under CALEA.<sup>61</sup> By maintaining this approach, the Commission will ensure that no TTP will be able to force its solution on the industry standards process. If law enforcement disagrees with an industry decision to exclude a TTP-provided capability from a standard, it can file a deficiency petition under section 107(b).

**C. The Industry Standards Process Plays the Lead Role in Defining CALEA Capability Requirements**

The Commission should reaffirm the central role of the industry-driven standards process in the development of CALEA compliance solutions. Since CALEA became law, industry organizations have spent thousands of hours (in cooperation with law enforcement) developing standards that provide the intercept capabilities mandated by CALEA in a manner that is realistic, efficient, and cost-effective for providers. Although packet-mode standards are less advanced than circuit-mode standards – in part because the regulatory status of services like broadband access and VoIP is only now being addressed in this proceeding – there are already a number of important packet-mode standards, including the Telecommunications Industry Association / Alliance for Telecommunications Industry Solutions J-STD-025-B standard and the CableLabs<sup>®</sup> PacketCable standard.

As an initial matter, the Commission should abandon the notion – raised but not endorsed in the *CALEA NPRM* – that the development of standards could be limited to organizations

---

<sup>61</sup> TTP solutions are analogous to 411 directory assistance (“DA”) services. Carriers are not required to provide DA service, but there is nevertheless competition among several independent DA service providers. Similarly, TTP solutions should not be mandated, but TTP vendors should compete for the business of carriers seeking assistance in developing CALEA solutions.



recognized by the American National Standards Institute (“ANSI”).<sup>62</sup> This approach would contradict the language of CALEA, strike down several existing standards (including CableLabs standards),<sup>63</sup> and restrict future use of the standards process. CALEA specifically provides that standards may be developed by “an industry association *or* standard-setting organization”,<sup>64</sup> and Congress stated that “[t]he legislation provides that the telecommunications industry *itself* shall decide how to implement law enforcement’s requirements. [CALEA] allows industry associations *and* standard-setting bodies” to develop compliance solutions.<sup>65</sup> That is, CALEA explicitly allows non-ANSI-accredited organizations (and even entities that are not “standard-setting bodies” at all) to draft CALEA compliance standards. The Commission may not limit this authority conferred by Congress.

The Commission also requests comment on whether existing packet-mode standards are deficient.<sup>66</sup> This invitation to attack existing standards in a general proceeding, where only 30

---

<sup>62</sup> *CALEA NPRM* at ¶ 80.

<sup>63</sup> CableLabs is a non-accredited body that has developed a standard – the PacketCable Electronic Surveillance Specification – that is recognized and praised by law enforcement. *See Hearing on Law Enforcement Access to Communications Systems in the Digital Age Before the House Comm. on Energy and Commerce, Subcomm. on Telecommunications and the Internet*, 108th Cong. (2004) (statement of Dr. Richard R. Green, president and chief executive officer, Cable Television Laboratories, Inc.), available at [http://www.cablelabs.com/downloads/Testimony\\_090804.pdf](http://www.cablelabs.com/downloads/Testimony_090804.pdf) (last visited Oct. 18, 2004). It is important to note, however, that the CableLabs standard is not appropriate for all technology architectures, including, for example, DSL broadband access services. Further, unlike ANSI-recognized standards and standards developed by bodies such as TIA and ATIS, the CableLabs standards development process is not open to industry-wide input and consensus.

<sup>64</sup> 47 U.S.C. § 1006(a)(2) (emphasis added).

<sup>65</sup> *CALEA Legislative History* at 3499 (emphasis added).

<sup>66</sup> *CALEA NPRM* at ¶ 81.

days will be available for response, is prejudicial and procedurally improper. As the Commission notes, CALEA gives industry the lead in establishing standards, and provides that

if a Government agency or any other person believes that [CALEA compliance] standards are deficient, the agency or person may petition the Commission to establish, by rule, technical requirements or standards.<sup>67</sup>

Although the law enforcement petition underlying this proceeding claims in a sentence that all current packet-mode standards are deficient,<sup>68</sup> it fails to identify specific deficiencies in any standard, as would be needed to trigger a Section 107(b) proceeding. Furthermore, for many broadband access and most VoIP services, no standards exist because these services have been unregulated until the present proceeding.<sup>69</sup> Accordingly, to attempt to address deficiency of standards now would be to put the cart quite a distance before the horse. The Commission should allow the industry standards process to function as mandated by CALEA and (as discussed in section IV.A below) should allow sufficient time for this to occur.

Notwithstanding the above, US ISPA offers a few comments on the appropriate content of standards for packet-mode services, including future standards for broadband access and VoIP services, addressing some of the issues raised in the *CALEA NPRM*.<sup>70</sup>

First, pursuant to section 107(b), any capability requirements or standards established by the Commission must:

---

<sup>67</sup> 47 U.S.C. § 1006(b).

<sup>68</sup> United States Department of Justice, Federal Bureau of Investigation and Drug Enforcement Administration, Joint Petition for Expedited Rulemaking, RM-10865, at 35 (Mar. 10, 2004).

<sup>69</sup> Standards do exist for certain such services, including cable services covered by the PacketCable standard, and broadband access services over UMTS and cdma2000 wireless networks. *See id.* at ¶ 85.

<sup>70</sup> *CALEA NPRM* at ¶¶ 81-85.

- be cost-effective;
- protect the privacy and security of communications not authorized to be intercepted;
- minimize the cost on residential ratepayers;
- encourage the provision of new technologies and services; and
- provide a reasonable time and conditions for compliance.<sup>71</sup>

Second, standards are not deficient simply because they do not require ISPs to “break open” packets, for the reasons stated in section III.A above.

Third, capabilities required for one service (in particular, DDE) should only be required for a different service to the extent that they are reasonably available to providers of that service, again for the reasons stated above.

Fourth, the Commission may not require standard formats for delivering CALEA information to law enforcement. Both the legislative history of CALEA and the original understanding of CALEA put forward by the Department of Justice make clear that carriers may use whatever delivery format is most appropriate to their technology and network. The Commission recognized as much in its *Third Report and Order* when it rejected a law enforcement proposal to include a standardized delivery interface capability in the final industry standard.<sup>72</sup> Indeed, even law enforcement has previously conceded that standardized delivery

---

<sup>71</sup> 47 U.S.C. § 1006(b).

<sup>72</sup> *CALEA Third Report and Order* at 16852 ¶ 136 (noting that “as Assistant Attorney General Colgate stated in February 1998, ‘a single delivery interface is not mandated by CALEA.’”). *See also CALEA Legislative History* at 3502 (“If the communication at the point it is intercepted is digital, the carrier may provide the signal to law enforcement in digital form. Law enforcement is responsible for determining if a communication is voice, fax or data and for translating it into useable form.”). The Commission found that nothing in CALEA “would require that the number of interfaces be limited.” *CALEA Third Report and Order* at 16852 ¶ 136. The Commission did note that industry may eventually “reach agreement on a relatively limited number of delivery interfaces, which should serve to reduce costs to LEAs,” as digital technology evolves. *Id.*

formats are not required by CALEA.<sup>73</sup> Accordingly, a standard should not be judged deficient if it does not contain a standard format for delivery.

#### **IV. COMPLIANCE AND ENFORCEMENT ISSUES**

In addition to clarity about what new technologies are covered and what obligations it has imposed, the Commission should seek a regulatory framework that minimizes unnecessary burdens on previously unregulated industries, and on innovation generally.

##### **A. The Commission Must Set Realistic Compliance Deadlines**

If the Commission moves ahead with its tentative conclusions to subject many broadband access and VoIP services to CALEA, the deadlines for implementing CALEA capability obligations for such newly regulated services must take account of the major new obligations on Internet-based service providers. In particular, the deadlines must take account of (a) the length of the service and the software and equipment design cycles for new services and (b) the need to develop standards for CALEA compliance for these services.

Law enforcement proposes a 15-month compliance deadline for newly regulated entities to come into compliance, and the Commission even asks whether the timeline should be shorter (with the opportunity for providers to file extension petitions).<sup>74</sup> These proposals fail to take into account realistic service, equipment and software design cycles, or associated standards processes. As industry participants commented regarding the law enforcement petition

---

<sup>73</sup> Federal Bureau of Investigation and Department of Justice, *In re Establishment of Technical Requirements and Standards for Telecommunications Carrier Assistance Capabilities Under the Communications Assistance for Law Enforcement Act*, Joint Petition for Expedited Rulemaking, CC Dkt. No. 97-213, at 57 (Mar. 27, 1998) (“Section 103 does not obligate carriers to use any particular interface protocol, and [DoJ and the FBI] are not asking the Commission to impose such an obligation by rule.”).

<sup>74</sup> *CALEA NPRM* at ¶ 143.

underlying the present *CALEA NPRM*, “benchmarks do not reflect how CALEA standards and solutions are developed in the real world, or otherwise realistically address the particular difficulties associated with developing standards and solutions for packet-mode technologies and services.”<sup>75</sup>

Congress recognized that CALEA compliance cannot be a rapid process of implementation, especially where new technologies are being introduced. Sections 104(b) and 111 of CALEA gave circuit-mode service providers four years to comply with the statute.<sup>76</sup> In the *CALEA NPRM*, the Commission has proposed to subject entirely new services to CALEA’s requirements; providers of such newly regulated services should be given a time period for compliance similar to the one that common carriers received in 1994. Indeed, providing CALEA solutions for packet-mode communications is a potentially more difficult process than providing circuit-switched CALEA capability. As the Commission notes in the *CALEA NPRM*, “in a circuit-based technology environment ... a relatively standardized, switch-based technology could be readily retrofitted or otherwise modified (and largely with funding provided directly by DoJ/FBI).”<sup>77</sup> In contrast, “the requirements of rapidly evolving packet-based technologies and architectures” create different demands on providers.<sup>78</sup>

For delivery of communications content, which must be provided for any services covered by CALEA, the 15-month compliance deadline proposed by law enforcement is a bare

---

<sup>75</sup> *Id.* at ¶ 107 & n. 248 (citing, for example, AT&T Comments at 9, 19-21; BellSouth Comments at 13-14; NTCA Comments at 2-3; SBC Comments at 18-19; and USTA Reply Comments at 4-6).

<sup>76</sup> 47 U.S.C. §§ 1001 note, 1003(b)(1).

<sup>77</sup> *CALEA NPRM* at ¶ 102.

<sup>78</sup> *Id.*

minimum. As the Commission tentatively concludes in the *CALEA NPRM*, however, the intermediate procedures and requirements that law enforcement suggests are unnecessary.<sup>79</sup>

For delivery of CII, for which obligations remain entirely unclear, a longer implementation period – at least three years – is needed so that standards and software may be developed.<sup>80</sup> If the implementation period is too short, new Internet-based services will be developed without knowing what CALEA obligations apply, producing substantial market disruption, interference with deployment of new services, and unnecessary cost and inefficiency. In particular, a period shorter than three years would be manifestly insufficient for products to be built to CALEA compliance standards that remain under development. Furthermore, the development of such standards must be coordinated with service providers' negotiations with manufacturers and TTPs to develop CALEA solutions.

The *CALEA NPRM* suggests that short compliance deadlines (and restricted deadline extensions) “could be precisely what Congress intended, because it would encourage carriers to press for the development of CALEA standards by industry-staffed committees and for solutions from manufacturers.”<sup>81</sup> US ISPA agrees that rapid standards processes should be encouraged, but this goal does not provide a justification for setting unrealistically tight compliance deadlines. In order to encourage prompt industry action while avoiding market disruption and inefficiency, the Commission should set a realistic date certain for CALEA compliance that is at

---

<sup>79</sup> *CALEA NPRM* at ¶ 91 (“[W]e believe that Law Enforcement’s goal can be achieved without us imposing the implementation deadlines and benchmark filings it requests.”).

<sup>80</sup> Where a relevant standard already exists, an appropriate deadline for CII would be three years from the date of adoption of the standard (or 18 months from the Commission’s final decision, if that period is shorter).

<sup>81</sup> *Id.* at ¶ 99.

least 15 months from the effective date of its order for call content and at least three years from the effective date for CII.

**B. Title III Plainly Authorizes Recovery of CALEA-Related Intercept Costs**

The *CALEA NPRM* also asks whether the Commission “should distinguish carrier recovery of CALEA-incurred capital costs generally from recovery of specific intercept-related costs”<sup>82</sup> for purposes of Title III of the Omnibus Crime Control and Safe Streets Act of 1968<sup>83</sup> (“Title III”). Quite simply, the Commission lacks statutory authority to draw such a distinction. More fundamentally, there is no statutory basis for the Commission to regulate in this area – an area it has not directly regulated at any time since Title III was passed in 1968. Furthermore, the broadband access and VoIP services at issue in this proceeding are services over which the Commission asserts no authority to regulate rates under the Communications Act – and such authority manifestly does not exist under CALEA.

The Commission seeks comment on law enforcement’s request for the Commission to establish rules requiring carriers to bear “sole financial responsibility” for implementing CALEA solutions for post January 1, 1995 communications equipment, facilities, and services.<sup>84</sup> The Commission should firmly reject this interpretation. The allocation in CALEA of a specific fund of \$500 million for reimbursement of CALEA compliance costs<sup>85</sup> did not abrogate the existing authority for carriers to recover their intercept costs under Title III. Where Congress intends to

---

<sup>82</sup> *Id.* at ¶ 132.

<sup>83</sup> Pub. L. 90-351, 82 Stat. 212 (1968) (codified, as amended, at 18 U.S.C. §§ 2510 *et seq.*)).

<sup>84</sup> *CALEA NPRM* at ¶ 119.

<sup>85</sup> 47 U.S.C. § 1009.

repeal a prior statute (in whole or in part), it must do so expressly,<sup>86</sup> which CALEA certainly does not do with respect to Title III.

Title III requires that “[a]ny provider of wire or electronic communication service ... or other person furnishing such facilities or technical assistance shall be compensated therefor by the applicant for reasonable expenses incurred in providing such facilities or assistance.”<sup>87</sup> And Title III places the authority for determining whether cost recovery is appropriate squarely in the hands of federal courts.<sup>88</sup> To our knowledge, no law enforcement agency has ever challenged a carrier’s request for cost recovery in the judicial forum that Title III provides – even though we understand that carriers have long charged CALEA costs as part of their “reasonable expenses” under Title III.

The Commission recognized this long-standing cost recovery policy in its *Order on Remand* when it stated that

carriers can recover at least a portion of their CALEA software and hardware costs by charging to [law enforcement agencies], for each electronic surveillance order authorized by CALEA, a fee that includes recovery of capital costs, as well as recovery of the specific costs associated with each order.<sup>89</sup>

---

<sup>86</sup> See, e.g., *Morton v. Mancari*, 417 U.S. 535, 550 (1974) (“In the absence of some affirmative showing of an intention to repeal, the only permissible justification for a repeal by implication is when the earlier and later statutes are irreconcilable.”); *Universal Interpretive Shuttle Corp. v. Washington Metropolitan Area Transit Comm’n, et al*, 393 U.S. 186, 193 (1968) (“There is thus no reason to ignore the principle that repeals by implication are not favored.”); *Gallenstein v. United States*, 975 F.2d 286, 290 (6th Cir. 1992) (“An express repeal requires that Congress overtly state with specificity that the subsequent statute repeals a portion of the former statute.”).

<sup>87</sup> 18 U.S.C. § 2518(4).

<sup>88</sup> *Id.*

<sup>89</sup> *CALEA Order on Remand* at 6917 ¶ 60.



There is no basis for reversing this decision a mere two years later. Citing its prior statement, the Commission in the *CALEA NPRM* recognizes that “[a]s a general rule, LEAs must compensate carriers for *their costs associated with provisioning a court-authorized intercept*.”<sup>90</sup>

That is the principle that should apply here. CALEA compliance costs are one of the main costs of provisioning intercepts for law enforcement. There is no principled way to distinguish between costs of implementing an overall CALEA compliance solution and costs associated with a particular intercept. To do so would be akin to arguing that depreciation of a Boeing 777 is not one of the costs that an airline bears when its plane flies from New York to Los Angeles.

Further, the Commission has no authority under Section 229(a) of the Communications Act or under CALEA itself to issue regulations governing cost recovery. Although Section 229(a) allows the Commission to prescribe rules to implement CALEA’s requirements,<sup>91</sup> it does not allow the Commission to interpret Title III or to implement regulations that undercut the intent of a statute enacted 25 years before CALEA.

The Congressional decision, reflected in Title III, that intercept provisioning costs should be borne by the public fisc is an entirely reasonable one. Effectively, this approach shifts intercept provisioning costs from telecommunications ratepayers to the public at large – which makes eminent sense given that the work of law enforcement benefits the entire public, rather than just users of particular telecommunications services. If this statutory rule were changed, the

---

<sup>90</sup> *CALEA NPRM* at ¶ 132 (emphasis added). The mere fact that the Commission has described the application of Title III in the CALEA context in these proceedings certainly does not give it direct regulatory authority under Title III.

<sup>91</sup> 47 U.S.C. § 229(a).

burden of these costs would be placed on operators of emerging packet-mode services and their customers, thereby impairing the viability of these new services. This would be contrary to the goal of CALEA “to avoid impeding the development of new communications services and technologies,”<sup>92</sup> and to the broader Commission policy of promoting development of new technologies.

The Commission also asks “whether recovery for capital costs associated with intercept provisioning should be different in the circuit-mode and packet-mode contexts.”<sup>93</sup> Again, the Commission lacks authority under Title III or CALEA to draw such a distinction. What’s more, any distinction between the two technologies should favor a more generous cost recovery policy for packet-mode technologies. There is no CALEA-authorized reimbursement fund for packet-mode infrastructure, not because Congress excluded that industry from reimbursement, but because Congress had no intent to impose CALEA on the industry. To impose new obligations while offering less opportunity to recover the cost of those obligations would be doubly unjust.<sup>94</sup> Yet the Commission has proposed to do just that. It would substantially restrict cost recovery options under CALEA, for example by tightening the standards for granting Section 109 “reasonably achievable” petitions.<sup>95</sup> Having done so, the Commission has an added obligation to allow appropriate CALEA costs to be charged to law enforcement (and the public) under Title III.

---

<sup>92</sup> *CALEA Legislative History* at 3493.

<sup>93</sup> *CALEA NPRM* at ¶ 133.

<sup>94</sup> 47 U.S.C. § 1009.

<sup>95</sup> *CALEA NPRM* at ¶ 98.

### **C. The Federal Courts Have Responsibility for CALEA Enforcement**

The *CALEA NPRM* also seeks comment on CALEA enforcement, asking whether the Commission should adopt the requirements of section 103 as Commission rules.<sup>96</sup> It should not. To do so would radically transform the balance envisioned by Congress.

CALEA makes clear that the federal courts have responsibility for enforcing CALEA's requirements. This is not mere formalism. The enforcement scheme is part of an overall balance that seeks to preserve innovation by the private sector and that puts the burden on law enforcement to demonstrate that it has been harmed before the innovator can be compelled to modify his product.

Any attempt by the Commission to assert its regulatory authority in the enforcement area oversteps the bounds of the statute. It is a fundamental precept of administrative law that "an agency literally has no power to act ... unless and until Congress confers power upon it."<sup>97</sup> And CALEA limits the Commission's jurisdiction to specific areas, including (a) specifying which entities are subject to CALEA,<sup>98</sup> (b) assessing CALEA compliance standards (and providing standards where appropriate),<sup>99</sup> and (c) establishing carrier security procedures.<sup>100</sup> By specifying the powers of the Commission under CALEA, "Congress effectively has provided a 'who, what,

---

<sup>96</sup> *Id.* at ¶¶ 115-116.

<sup>97</sup> *Louisiana Pub. Serv. Comm'n v. FCC*, 476 U.S. 355, 374 (1986).

<sup>98</sup> 47 U.S.C. § 1001(8)(B)(ii), (C)(ii).

<sup>99</sup> *Id.* at § 1008(b)(1).

<sup>100</sup> *Id.* at § 1004.

when, and how’ laundry list governing the [Commission’s] authority.”<sup>101</sup> The D.C. Circuit has categorically dismissed the idea that an agency “possesses *plenary* authority to act within a given area simply because Congress has endowed it with *some* authority to act in that area.”<sup>102</sup> That is, any rules that the Commission adopts must be limited to areas in which it has authority to regulate.

With respect to remedies and enforcement, the Supreme Court has stated that “it is an elemental canon of statutory construction that where a statute expressly provides a particular remedy or remedies, a court must be chary of reading others into it.”<sup>103</sup> The federal courts have made it clear, particularly under the Telecommunications Act of 1996, that the Commission must apply telecommunications statutes as they are written.<sup>104</sup> Likewise, the Communication Act’s general grant of authority to the Commission does not allow it to ignore the court enforcement regime that Congress established.<sup>105</sup>

In particular, the Commission’s proposed enforcement approach ignores the statutory defenses available in CALEA enforcement actions. For example, under CALEA, a company cannot be sanctioned for deploying noncompliant equipment unless law enforcement proves that

---

<sup>101</sup> *Railway Labor Executives’ Ass’n v. National Mediation Bd.*, 29 F.3d 655, 667 (D.C. Cir. 1994) (en banc).

<sup>102</sup> *Id.* at 670 (original emphasis).

<sup>103</sup> *Transamerica Mortgage Advisors, Inc. v. Lewis*, 444 U.S. 11, 19 (1979). *See also American Bus Ass’n v. Slater*, 231 F.3d 1, 5 (D.C. Cir. 2000).

<sup>104</sup> *See, e.g., United States Telecom Ass’n v. FCC*, 359 F.3d 554 (D.C. Cir. 2004) (“*USTA II*”); *United States Telecom Ass’n v. FCC*, 290 F.3d 415 (D.C. Cir. 2002) (“*USTA I*”).

<sup>105</sup> *CALEA NPRM* at ¶ 116.

it has no alternative method of getting the information it seeks through the enforcement action.

Section 108 of CALEA plainly states that:

A court shall issue an order enforcing this title ... only if the court finds that (1) alternative technologies or capabilities or the facilities of another carrier are not reasonably available to law enforcement ... and (2) compliance with [CALEA's requirements] is reasonably achievable through the application of available technology to the equipment, facility, or service at issue or would have been reasonably achievable if timely action had been taken.<sup>106</sup>

This provision also allows innovators to bring their products to market without first negotiating a full CALEA compliance scheme with the FBI. Wiretaps are relatively rare in the United States,<sup>107</sup> and an innovator might decide to market a new product without a complete CALEA solution – trusting that a partial solution, combined with information available to law enforcement from other sources, would be sufficient in the unlikely event that a wiretap is needed in the first months of service. In those circumstances, the defenses to enforcement actions under CALEA are crucial protectors of innovation. The alternative – the prospect of an immediate cease-and-desist order and/or fine before any wiretap order has been served and before the first customer has signed up – will discourage all but the most confident innovator from going to market without a fully negotiated CALEA agreement with the FBI. The consequences for innovation, at least in the United States, will be severe.

---

<sup>106</sup> 47 U.S.C. § 1007(a). Further, Congress intended to limit the courts' authority to issue enforcement orders. "[T]he court must find that law enforcement is seeking to conduct its interception at the best, or most reasonable, place for such interception" and that compliance is reasonably achievable. *CALEA Legislative History* at 3508.

<sup>107</sup> In 2002, for example, a total of only 1,358 wiretap orders were issued in the United States, and only 1,273 wiretaps were installed. Of those number, 497 wiretap orders issued and 490 installed were authorized by federal judges. Only 19 states reported wiretap activity in 2002. Administrative Office of the United States Courts, *2002 Wiretap Report* at 7, tbl. 2 (April 2003), *available at* <http://www.uscourts.gov/wiretap02/contents.html>.

CALEA did not envision such an aggressive enforcement scheme. Section 229(a) of CALEA does authorize the Commission to prescribe “such rules as are necessary to implement the requirements of [CALEA].”<sup>108</sup> However, Section 229 is not a delegation of limitless power that allows the Commission to supersede the enforcement framework specified in CALEA’s text. Section 229(a) must be read through the lens of CALEA, including the expressly limited powers that CALEA assigns to the Commission. Furthermore, where Congress has separately delegated CALEA enforcement power, it has been quite explicit about that delegation. For example, 18 U.S.C. § 2252 provides authority for courts to enforce CALEA in connection with intercept orders and to assess civil penalties for CALEA violations. It would be indefensible for the Commission to rely on subtle differences between the definitions of “telecommunications carrier” under the Communications Act and CALEA but then to ignore the much clearer differences between the statutes with respect to enforcement.

In sum, basic principles of administrative law and statutory construction make quite clear that under CALEA, the courts bear sole enforcement responsibility that the Commission may not supplant.

## **V. CONCLUSION**


The proposals in the *CALEA NPRM* would effect a major extension of Commission regulation to Internet-based services. US ISPA acknowledges for purposes of this proceeding that extension of CALEA to certain broadband access and VoIP services may be appropriate. But the Commission must implement this new regulation in a manner that is faithful to the text and legislative history of CALEA and that achieves a fair balance between law enforcement

---

<sup>108</sup> 47 U.S.C. § 229.

interests and the important interests of privacy and development of new technologies. In these comments, US ISPA has sought to articulate concrete proposals on how this should be done. Perhaps most important, the Commission should define CII capability obligations for broadband access and VoIP services in a manner that recognizes the unique characteristics of these services and that does not require ISPs to “break open” packets and examine content not required for their operations.

Respectfully submitted,

A handwritten signature in black ink, appearing to read 'SASD', followed by a horizontal line.

United States Internet Service Provider  
Association

*Of Counsel:*

Stewart A. Baker  
Maury D. Shenk  
Emily Hancock  
Daniel C.H. Mah  
STEPTOE & JOHNSON LLP  
1330 Connecticut Avenue, NW  
Washington, DC 20036  
Tel: (202) 429-3000

Dated: November 8, 2004